CLAIMS

What is claimed is:

1. A method comprising:

sequentially storing a plurality of results provided by a stream cipher output rule in a first, second, and third storage units;

providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third storage units that are at least a threshold value apart; and

upon reaching the threshold value of the output rule results, serially rotating contents of the first, second, and third storage units.

2. A method as recited by claim 1, wherein a short-term correlation between the individual values from the first and third storage units are limited.

3. A method as recited by claim 1, wherein a length of each of the first, second, and third storage units equals the threshold value.

4. A method as recited by claim 1, wherein the first, second, and third storage units are implemented in a single memory device.

5. A method as recited by claim 1, wherein the serial rotation is performed by shifting the first, second, and third storage units in a same direction.

6. A method as recited by claim 1, wherein the pairing function results are stored in a table.

7. A method as recited by claim 1, wherein the method is utilized to strengthen an output of a stream cipher keystream generator.

8. A method as recited by claim 1, wherein only the first and third storage units are active at any given time.

9. A method as recited by claim 1, wherein the first and third storage units are initialized with random values.

10. A method as recited by claim 1, wherein the method is applied recursively.

11. A method as recited by claim 1, wherein the output rule is combined with one or more update rules selected from a group comprising random walks, T-functions, LFSRs (linear feedback shift registers), and word-based stream ciphers.

12. A method as recited by claim 11, wherein the random walks are selected from one or more walks in a group comprising an additive walk, a

multiplicative walk, a Gabber-Galil walk, a Ramanujan walk, a permutation walk, and a random walk with a dynamic generator.

13. A method as recited by claim 1, further comprising enhancing the pairing function by utilizing a fourth storage unit.

14. A method as recited by claim 13, wherein the fourth storage unit is walked through using a one-cycle secret permutation.

15. A method as recited by claim 14, wherein the secret permutation slowly mutates.

16. A method as recited by claim 13, wherein the fourth storage unit is initialized with random values.

17. A method as recited by claim 13, wherein the fourth storage unit is initialized with random values and a variable delay.

18. A system comprising:

a processor;

a system memory coupled to the processor;

sequentially storing a plurality of results provided by a stream cipher output rule in a first, second, and third portion of the system memory;

providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third portions of the system memory that are at least a threshold value apart; and

upon reaching the threshold value of the output rule results, serially rotating contents of the first, second, and third portions of the system memory.

19. A system as recited by claim 18, wherein a short-term correlation between the individual values from the first and third portions of the system memory are limited.

20. A system as recited by claim 18, wherein a length of each of the first, second, and third portions of the system memory equals the threshold value.

21. A system as recited by claim 18, wherein the first, second, and third portions are implemented in multiple memory devices.

22. A system as recited by claim 18, wherein the serial rotation is performed by shifting the first, second, and third portions in a same direction.

23. A system as recited by claim 18, wherein the pairing function results are stored in a table on the system memory.

24. A system as recited by claim 18, wherein the system is utilized to strengthen an output of a stream cipher keystream generator.

25. A system as recited by claim 18, wherein the first and third portions are initialized with random values.

26. A system as recited by claim 18, wherein the output rule is combined with one or more update rules selected from a group comprising random walks, T-functions, LFSRs (linear feedback shift registers), and word-based stream ciphers.

27. A system as recited by claim 26, wherein the random walks are selected from one or more walks in a group comprising an additive walk, a multiplicative walk, a Gabber-Galil walk, a Ramanujan walk, a permutation walk, and a random walk with a dynamic generator.

28. A system as recited by claim 18, wherein an operation of the pairing function is enhanced by utilizing a fourth portion of the system memory.

29. A system as recited by claim 28, wherein the fourth portion is initialized with random values.

30. A system as recited by claim 28, wherein the fourth portion is initialized with random values and a variable delay.

31. One or more computer-readable media having instructions stored thereon that, when executed, direct a machine to perform acts comprising:

sequentially storing a plurality of results provided by a stream cipher output rule in a first, second, and third storage units;

providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third storage units that are at least a threshold value apart; and

upon reaching the threshold value of the output rule results, serially rotating contents of the first, second, and third storage units.

32. One or more computer-readable media as recited by claim 31, wherein a short-term correlation between the individual values from the first and third storage units are limited.

33. One or more computer-readable media as recited by claim 31, wherein a length of each of the first, second, and third storage units equals the threshold value.

34. One or more computer-readable media as recited by claim 31, wherein the first, second, and third storage units are implemented in a single memory device.

35. One or more computer-readable media as recited by claim 31, wherein the serial rotation is performed by shifting the first, second, and third storage units in a same direction.

36. One or more computer-readable media as recited by claim 31, wherein the pairing function results are stored in a table.

37. One or more computer-readable media as recited by claim 31, wherein the acts are performed recursively.

38. One or more computer-readable media as recited by claim 31, wherein the output rule is combined with one or more update rules selected from a group comprising random walks, T-functions, LFSRs (linear feedback shift registers), and word-based stream ciphers.

39. One or more computer-readable media as recited by claim 38, wherein the random walks are selected from one or more walks in a group comprising an additive walk, a multiplicative walk, a Gabber-Galil walk, a Ramanujan walk, a permutation walk, and a random walk with a dynamic generator.

40. One or more computer-readable media as recited by claim 31, further comprising enhancing the pairing function by utilizing a fourth storage unit.